Patch Release Note

Patch 86261-04
For Rapier and AT-8800 Series Switches

Introduction

This patch release note lists the issues addressed and enhancements made in patch 86261-04 for Software Release 2.6.1 on existing models of Rapier and AT-8800 Series switches. Patch file details are listed in Table 1.

Table 1: Patch file details for Patch 86261-04.

Base Software Release File	86-261.rez
Patch Release Date	19-Nov-2003
Compressed Patch File Name	86261-04.paz
Compressed Patch File Size	261628 bytes

This release note should be read in conjunction with the following documents:

- Release Note: Software Release 2.6.1 for Rapier and AT-8800 Series Switches (Document Number C613-10383-00 Rev A) available from *www.alliedtelesyn.co.nz/documentation/documentation.html*.
- Rapier Series Switch or AT-8800 Series Switch Documentation Set for Software Release 2.6.1 available on the Documentation and Tools CD-ROM packaged with your switch, or from *www.alliedtelesyn.co.nz/documentation/documentation.html*.

WARNING: Using a patch for a different model or software release may cause unpredictable results, including disruption to the network. Information in this release note is subject to change without notice and does not represent a commitment on the part of Allied Telesyn International. While every effort has been made to ensure that the information contained within this document and the features and changes described are accurate, Allied Telesyn International can not accept any type of liability for errors in, or omissions arising from the use of this information.

Some of the issues addressed in this Release Note include a level number. This number reflects the importance of the issue that has been resolved. The levels are:

Level 1 This issue will cause significant interruption to network services, and there is no work-around.

Level 2 This issue will cause interruption to network service, however there is a work-around.

Level 3 This issue will seldom appear, and will cause minor inconvenience.

Level 4 This issue represents a cosmetic change and does not affect network operation.

Features in 86261-04

Patch 86261-04 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 03910 Module: IPG Level: 3

When RIP demand mode was enabled, and one interface changed to a reachable state, the triggered *Request* packet was not sent from that interface, and triggered *Response* packets were not sent from all other RIP interfaces. This resulted in slow convergence of routing tables across the network. This issue has been resolved.

PCR: 03927 Module: BRI

Support has been added for the AT-AR021 (S) BRI-S/T PIC (Port Interface Card) with basic rate ISDN.

PCR: 03967 Module: IPG Level: 2

RIP did not send the correct next hop address if the route originated from a different subnet to that of the egress interface. This issue has been resolved.

PCR: 03970 Module: IPV6 Level: 3

If an IPv6 filter that blocked traffic on a VLAN interface was removed, the traffic was still blocked. This issue has been resolved.

PCR: 03978 Module: OSPF Level: 3

Occasionally an error occurred with OSPF's route table calculation, so all routes in the network were not discovered. The error only happened with a network topology that involved connections between routers via both a Point to Point link and a transit network link. This issue has been resolved. A new command has been added that forces a route table recalculation by rerunning the Shortest Path First calculation. The command is:

```
RESET OSPF SPF [DEBUG]
```

If DEBUG is specified, debugging information for the route table calculation is output to the port from which the command was executed. SPF debugging can be turned on for every route table calculation using the ENABLE OSPF DEBUG=SPF command, but this will be overridden if DEBUG is specified with the RESET OSPF SPF command.

PCR: 31009 Module: HTTP Level: 3

The server string was not copied correctly into an HTTP file request when loading information from the configuration script. This issue has been resolved.

PCR: 31064 Module: SWI Level: 2

When 10/100 copper ports were disabled with the DISABLE SWITCH PORT command, their link state was still UP. This issue has been resolved.

PCR: 31072 Module: SWI Level: 3

If the DISABLE SWITCH PORT command appeared in the configuration script, an interface could come up even though *ifAdminStatus* was set to 'down'. This issue has been resolved.

PCR: 31084 Module: IPV6 Level: 2

A fatal error sometimes occurred because of incorrect responses to Neighbour Solicitation messages. This issue has been resolved.

PCR: 31093 Module: SWI Level: 1

If a switch port was disabled on a switch running STP, traffic was sometimes not passed through that port after it was re-enabled. This issue has been resolved.

PCR: 31096 Module: FFS Level: 3

The SHOW FILE command caused an error when the displayed file had a duplicate entry due to file size mismatch. This issue has been resolved. An error message is now logged when the SHOW FILE command detects a duplicate file. The first FFS file will be deleted when a duplicate exists.

PCR: 31098 Module: DHCP Level: 3

Static DHCP address ranges were not reclaimed if the *Reclaim* operation was interrupted by the interface going down. This issue has been resolved.

PCR: 31100 Module: L2TP Level: 3

An error occurred in L2TP when call names consisted of numeric characters only. This issue has been resolved. The ADD L2TP CALL command now only accepts call names that contain at least one alphabetic character.

PCR: 31119 Module: LOG Level: 2

The maximum value that the MESSAGES parameter accepted for the CREATE LOG OUTPUT command was different from the value that could be set with the SET LOG OUTPUT command. The DESTROY LOG OUTPUT command did not release the NVS memory that was reserved for the output. These issues have been resolved.

PCR: 31132 Module: DHCP Level: 2

The DHCP server did not take any action when it received a DHCP *decline* packet. This was because the device only checked the *ciaddr* field in the packet, and not the *RequestedIPAddress* option. This issue has been resolved.

PCR: 31133 Module: IPG

This PCR introduces an enhancement that extends an issue that was resolved in PCR 03890, in which switch port entries are only created for special router multicast addresses. It is now possible to specify reserved multicast addresses that will be treated as multicast packets from routers. Use the following commands to configure this feature.

ADD IGMPSNOOPING ROUTERADDRESS

Syntax

```
ADD IGMPSNOOPING ROUTERADDRESS=ipaddr[,...]
```

Description

where:

- *ipaddr* is a reserved IP multicast address in dotted decimal notation.

This command adds reserved IP multicast addresses to the list of router multicast addresses. The IP address specified must be within the range 224.0.0.1 to 224.0.0.255. This command is only valid if the IGMP snooping router mode is set to IP with the SET IGMPSNOOPING ROUTERMODE command.

SET IGMPSNOOPING ROUTERMODE

Syntax

```
SET IGMPSNOOPING ROUTERMODE=
    {ALL|DEFAULT|IP|MULTICASTROUTER|NONE}
```

Description

This command sets the mode of operation for IGMP Snooping.

If ALL is specified, all reserved multicast addresses (i.e. 2240.0.1 to 224.0.0.255) are treated as router multicast addresses.

If DEFAULT is specified, the following addresses are treated as router multicast addresses:

- IGMP Query: 224.0.0.1
- All routers on this subnet: 224.0.0.2
- DVMRP Routers: 224.0.0.4
- OSPFIGP all routers: 224.0.0.5
- OSPFIGP designated routers: 224.0.0.6
- RIP2 routers: 224.0.0.9
- All PIM routers: 224.0.0.13
- All CBT routers: 224.0.0.15

If IP is specified, addresses that are treated as router multicast addresses are specified with the ADD/DELETE IGMPSNOOPING ROUTERADDRESS command. In this mode, the switch will retain previous addresses that have already been specified.

If MULTICAST is specified, the following addresses are treated as router multicast addresses:

- DVMRP Routers: 224.0.0.4
- All PIM routers: 224.0.0.13

If NONE is specified, no router ports are created.

DELETE IGMPSNOOPING ROUTERADDRESS

Syntax `DELETE IGMPSNOOPING ROUTERADDRESS=ipaddr[,...]`

where

- *ipaddr* is a reserved IP multicast address in dotted decimal notation.

Description This command deletes reserved IP multicast addresses from the list of router multicast addresses. The IP address specified must be within the range 224.0.0.1 to 224.0.0.255. This command is only valid if the IGMP snooping router mode is set to IP with the SET IGMPSNOOPING ROUTERMODE command.

SHOW IGMPSNOOPING ROUTERADDRESS

Syntax `SHOW IGMPSNOOPING ROUTERADDRESS`

Description This command displays information about the list of configured IP multicast router addresses currently configured on the switch (Figure 1).

Figure 1: Example output for SHOW IGMPSNOOPING ROUTERADDRESS

```
IGMP Snooping Router Address
-------------------------------------------------------------------------------
IGMP Snooping Router Mode ..... IP

Router Address List
-------------------------------
224.0.0.4
224.0.0.6
224.0.0.80
224.0.0.43
224.0.0.23
224.0.0.15
224.0.0.60
-------------------------------------------------------------------------------
```

PCR: 31134 Module: RSTP Level: 2

Bridges transmitted BPDUs at the rate specified by the local *helloTime* value when they were not the root bridge. This is the behaviour specified in 802.1w-2001. This behaviour can cause instability in the spanning tree when bridges are configured with different *helloTime* values, especially when the root bridge's *helloTime* is significantly less than other bridges in the tree. This issue has been resolved. Non-root bridges now adopt the root bridge's *helloTime* value propagated in BPDUs.

PCR: 31135 Module: IPV6 Level: 3

The ADD IPV6 HOST command accepted an invalid IPv6 address. This issue has been resolved.

PCR: 31140 Module: FIREWALL Level: 4

The firewall sent an erroneous IPSPOOF attack message when processing large packets. This issue has been resolved.

PCR: 31145 Module: SWI Level: 3

The port counters were not incremented:

- *ifInDiscards*
- *ifinErrors*
- *ifOutDiscards*
- *ifOutErrors*

This issue has been resolved.

PCR: 31146 Module: SWI Level: 3

The following SNMP MIB objects could not be set:

- *Dot1dStpPriority*
- *Dot1dStpBridgeMaxAge*
- *Dot1dStpBridgeHelloTime*
- *Dot1dStpBridgeForwardDelay*

This issue has been resolved.

PCR: 31147 Module: DHCP Level: 3

DHCP was incorrectly using the directly connected network interface source IP address as the source IP address of packets it generates. This issue has been resolved. DHCP now uses the local IP address as the source address for the packets it generates when a local IP interface address is set. If a local IP interface address is not set, then it uses the IP address of the interface where packets are sent from as the source address.

PCR: 31148 Module: PIM, PIM6 Level: 2

When the device rebooted with PIM or PIM6 enabled, it sometimes did not send a *Hello* packet quickly enough. This issue has been resolved.

PCR: 31152 Module: DHCP Level: 2

When a DHCP client was in the renewing state, and it sent a DHCP *Request*, the device did not add the ARP entry to the ARP table. Instead, the device generated an ARP *Request* in order to transmit the DHCP *Ack*. This caused a broadcast storm in the network when the client kept sending DHCP *Request*s. This issue occurred because the *ciaddr* field, not the *giaddr* field, was checked in the *Request* packet when the device determined whether to add the ARP entry. This issue has been resolved.

PCR: 31153 Module: IPG Level: 4

In the output of the SHOW IP DNS CACHE command, "TTL" was displayed as seconds. This has been changed to minutes because the TTL is updated every minute.

PCR: 31154 Module: STP Level: 4

The current implementation of RSTP conforms to the IEEE standard 802.1w-2001. However, several minor deviations from the standard are possible without having a functional impact on the behaviour of RSTP. These changes are useful for debugging RSTP, and tidy up aspects of RSTP that sometimes have no purpose. The following three variations have been implemented:

- The *Learning* and *Forwarding* flags are set in BPDUs to indicate the state of the Port State Transition state machine.
- The *Agreement* flag is set in BPDUs only when a Root Port is explicitly agreeing to a proposal from a designated port. Do not set the *Agreement* flag in BPDUs transmitted by Designated Ports.
- The *Proposal* flag is not set in a BPDU sent by a designated port once the port has reached the forwarding state.

PCR: 31158 Module: CORE Level: 3

On AT-8800 series switches, when the fan status changed, the device did not send a SNMP trap and log. When the temperature was above the allowable threshold, the device sent the wrong SNMP trap. This issue has been resolved. Also, the temperature thresholds of the AT-8824 and AT-8848 have been set to different values of 62° C and 67° C respectively.

PCR: 31159 Module: FW, VLAN Level: 2

Static ARP entries sometimes prevented the firewall from working correctly. This is because when an VLAN interface is added to the firewall, the CPU takes over the routing from the switch silicon in order to inspect the packet. Hence all the Layer 3 route entries must be deleted. However, static ARP Layer 3 entries were not being deleted from the silicon. This issue has been resolved. When interface is added to the firewall, all hardware layer 3 routing is now turned off to allow the firewall to inspect packets.

PCR: 31161 Module: LOG Level: 3

If the number of messages to be stored in the TEMPORARY log output was changed with the SET LOG OUTPUT MESSAGE command, the SHOW LOG command output did not return any matching log messages. This issue has been resolved. Existing messages are now displayed.

PCR: 31162 Module: SWI Level: 2

A STP topology change incorrectly deleted static ARP entries. This issue has been resolved.

PCR: 31167 Module: IPG Level: 2

IP MVR member ports were not timing out. MVR member ports now timeout in the same way as IP IGMP ports. The timeout values are configured by IGMP. Also, IGMP interfaces were incorrectly being enabled and disabled by MVR. This issue has been resolved.

PCR: 31170 Module: SWI Level: 2

After an AT-8800 series switch was powered down or rebooted, non-auto negotiating copper GBICs were not handled correctly. This issue has been resolved.

PCR: 31171 Module: PORTAUTH, USER,STP Level: 2

This PCR enhances the robustness of the 802.1x port authentication protocol.

PCR: 31174 Module: IPG Level: 2

If a device had IPSec and firewall enabled, it could not handle long ICMP packets even when enhanced fragment handling was enabled on the firewall. If a long packet is passed to the firewall for processing, the firewall chains the fragmented packets. The firewall can process chained packets, but IPSec could not process these packets, and dropped them. This was only an issue for packets between 1723 and 1799 bytes long. This issue has been resolved. The way IP processes fragmented packets has been changed so that IPsec no longer drops chained packets.

PCR: 31179 Module: SWI Level: 3

Addresses learned with static port security were not added to the configuration when the CREATE CONFIG command was executed. This issue has been resolved.

PCR: 31180 Module: USER Level: 2

The following commands did not require security officer privilege when the device was in security mode, but this privilege should have been required:

- ADD USER
- SET USER
- DELETE USER
- PURGE USER
- ENABLE USER
- DISABLE USER
- RESET USER

This issue has been resolved. Security officer privilege is now required for these commands when security mode is enabled with the ENABLE SYSTEM SECURITY_MODE command.

PCR: 31184 Module: SW56 Level: 2

Some issues occurred on 48 port Rapier series switches when MAC addresses were learned and then relearned on a different port. These issues have been resolved.

PCR: 31185 Module: SWI Level: 2

Tagged ports did not tag packets received from the bridge before transmitting them. This issue has been resolved.

PCR: 31190 Module: SWI, SW56 Level: 2

When static port security was enabled with the RELEARN parameter in the SET SWITCH PORT command, and a switch port was reset or unplugged, the MAC entries were removed (unlearned) from the forwarding database table. The MAC entries should only be removed when dynamic port security is in use. This issue has been resolved.

PCR: 31191 Module: PORTAUTH, USER Level: 2

A device in a supplicant role failed to authenticate if it used EAP-MD5 encryption with Windows 2000 or 2003 Server as the RADIUS server. Also, a fatal error occurred if the device received EAPOL packets containing a very large value in the packet length field. These issues have been resolved.

PCR: 31192 Module: LOG Level: 3

Syslog entries did not contain the date, time and unique identifier of the message source. This issue has been resolved. The CREATE LOG OUTPUT and SET LOG OUTPUT commands have been modified to control whether or not this information is included.

The following parameter has been added to the CREATE LOG OUTPUT and SET LOG OUTPUT commands:

```
[SYSLOGFORMAT=NORMAL|EXTENDED]
```

If the SYSLOGFORMAT parameter is set to EXTENDED the date, time and unique identifier of message source are included in the syslog message. If the parameter is set to NORMAL, this information is not included in the syslog message. The default is NORMAL.

PCR: 31193 Module: IPG Level: 2

When IP multicasting was not enabled, all IP multicast packets were passed to the CPU, causing overloading. This issue has been resolved. Now, if IP multicasting is not enabled, these packets are not sent to the CPU.

PCR: 31194 Module: BGP, IP Level: 3

When executing the command:

```
ADD IP ROUTEMAP ENTRY SET ASPATH
```

followed by the command:

```
ADD IP ROUTEMAP ENTRY COMMUNITY ADD=YES
```

where the values for ROUTEMAP and ENTRY were the same in both commands, the second command failed and returned a "`ROUTEMAP clause already exists`" error message. This issue has been resolved.

PCR: 31201 Module: SW56, SWI Level: 2

Fibre GBICs on Rapier and AT-8800 series switches sometimes did not establish a link when powered on for the first time. This issue has been resolved.

PCR: 31205 Module: VRRP Level: 3

Two VRRP log messages were displayed when they should not have been. The log messages were:

```
Vrrp 1: Vlan vlan2 10 Port Failed decrementing priority by 20

Vrrp 1: Vlan vlan2 1 Port up incrementing priority by 2
```

This issue has been resolved. These messages are now displayed at the correct time.

PCR: 31215 Module: SNMP Level: 4

The entry for the *FanAndPs* group in the private MIB did not return valid information. This issue has been resolved.

PCR: 31221 Module: SW56 Level: 1

On AT-8848 switches, a STP loop occurred if the Gigabit uplink port 49 was in the blocking state. This issue has been resolved.

PCR: 31237 Module: CORE Level: 3

Sometimes the initialisation of fan and temperature monitoring was delayed, and this was reported as a failure. This issue has been resolved. The delay was temporary and is no longer reported as a failure.

Features in 86261-03

Patch file details are listed in Table 2:

Table 2: Patch file details for Patch 86261-03.

Base Software Release File	86-261.rez
Patch Release Date	7-Nov-2003
Compressed Patch File Name	86261-03.paz
Compressed Patch File Size	176500 bytes

Patch 86261-03 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 31164 Module: SWI Level: 2

On AT-8800 Series switches, fibre GBICs were treated like copper GBICs if the switch had been powered off for more than one minute. This issue has been resolved.

Features in 86261-02

Patch file details are listed in Table 3:

Table 3: Patch file details for Patch 86261-02.

Base Software Release File	86-261.rez
Patch Release Date	3-Nov-2003
Compressed Patch File Name	86261-02.paz
Compressed Patch File Size	384839 bytes

Patch 86261-02 includes all issues resolved and enhancements released in previous patches for Software Release 2.6.1, and the following enhancements:

PCR: 03726 Module: TTY, USER Level: 3

The time recorded when a user logged in was overwritten when the same user logged in a second time while the original connection was still active. This meant the SHOW USER command displayed the same time for both connections. This issue has been resolved.

PCR: 03781 Module: STP Level: 2

A buffer leak occurred when rapid STP was specified with the SET STP MODE=RAPID command, but STP had not been enabled with the ENABLE STP command. This issue has been resolved.

PCR: 03855 Module: IPG Level: 2

Previously, an IP multicast stream destined for an IP multicast group was forwarded out ports in the All Groups IGMP snooping entry even after this entry had timed out. This issue has been resolved.

PCR: 03861 Module: IPV6 Level: 2

When a connector was plugged into one physical interface, the RIPng request packet was erroneously transmitted from all interfaces on the switch. This issue has been resolved.

PCR: 03873 Module: IPG Level: 4

The STATIC and INTERFACE options have been removed from the PROTOCOL parameter in the ADD IP ROUTE FILTER and SET IP ROUTE FILTER commands. These parameters were redundant because received static and interface routes are always added to the route table.

PCR: 03890 Module: IGMP, SWI Level: 2

The switch was adding a router port for multicast packets to destinations with an address in the range 224.0.0.x. Switch port entries are now only created for special router multicast addresses.

PCR: 03905 Module: TTY Level: 3

A fatal error occurred in the text editor while selecting blocks and scrolling up. This issue has been resolved.

PCR: 03926 Module: PIM Level: 2

Repeated *Assert* messages were sent after the prune limit expired. This issue has been resolved. The default dense mode prune hold time has been changed from 60 seconds to 210 seconds.

PCR: 03932 Module: PING Level: 3

The ADD PING POLL command had a duplicate entry for the LENGTH parameter in the dynamic PING configuration if LENGTH was not the default value. This generated an incorrect configuration file when the CREATE CONFIG command was executed. This issue has been resolved.

PCR: 03935 Module: ISAKMP Level: 3

ISAKMP debug messages now correctly output IPv6 addresses when using IPv6, and IPv4 addresses when using IPv4.

PCR: 03937 Module: IPSEC Level: 2

The IP version of packets was not being checked, so an IPv4 packet could match an IPv6 IPSec policy. This issue has been resolved.

PCR: 03940 Module: PKI Level: 1

The following two issues have been resolved:

- Large CRL files were not decoded correctly.
- The certificate database was not validated immediately after the CRL file was updated.

PCR: 03941 Module: FIREWALL Level: 2

TCP *Keepalive* packets for FTP sessions were passing through the firewall during the TCP setup stage with TCP Setup Proxy enabled. *Keepalive* packets include sequence numbers that have already been acknowledged. Such packets now fail stateful inspections and are dropped by the FTP application-level gateway.

PCR: 03954 Module: IPV6 Level: 2

An anycast address could not be assigned when the prefix for the anycast address had previously been assigned on that interface. This issue has been resolved.

PCR: 03958 Module: FIREWALL Level: 2

The ADD FIREWALL POLICY RULE and SET FIREWALL POLICY RULE commands no longer accept the GBLREMOTEIP parameter with standard NAT, or enhanced NAT for a private interface.

PCR: 03965 Module: IPSEC Level: 3

IPv6 used the same SA soft expiry timer at both ends of a link, which used memory unnecessarily. This issue has been resolved.

PCR: 03973 Module: IPG Level: 3

When equal cost multipath routes were used, the IP option field for trace route was not applied correctly. This issue has been resolved.

PCR: 03974 Module: IPG Level: 3

The IP filter blocked ping packets when the ACTION for these was set to INCLUDE with the ADD IP FILTER command. This issue was caused by the default SMASK value of 255.255.255.255, which blocked all incoming packets. This issue has been resolved.

PCR: 03982 Module: FIREWALL Level: 3

The SMTP proxy did not correctly filter sessions where messages were fragmented. This had the potential to prevent the detection of third-party relay attacks. This issue has been resolved.

PCR: 03986 Module: BGP, IPG Level: 2

Route flapping occurred if an interface went down and there was another route to that interface's next hop. This issue has been resolved.

PCR: 03993 Module: FIREWALL Level: 4

The AUTHENTICATION parameter has been removed from the "?" CLI help for firewall commands. This was not a valid parameter.

PCR: 03994 Module: SWI Level: 2

Port speed and duplex values set with the SET SWITCH PORT SPEED command were sometimes not applied correctly. This issue has been resolved.

PCR: 03996 Module: FIREWALL Level: 2

Occasionally some firewall timers stopped early, resulting in sessions being removed prematurely. Because of this, TCP *Reset* packets could be sent by the firewall before TCP sessions were finished. This issue has been resolved.

PCR: 31001 Module: DHCP Level: 2

When executing the SET DHCP POLICY, DELETE DHCP POLICY and DESTROY DHCP POLICY commands, memory was not de-allocated correctly. This issue has been resolved.

PCR: 31002 Module: UTILITY Level: 2

Sometimes the device rebooted when a severe multicast storm occurred due to a loop in the network. This issue has been resolved.

PCR: 31012 Module: PIM Level: 2

The *prune* time limit was not being cancelled when an IGMP join was received by the switch. This was forcing the switch to send a *Graft* message in the upstream direction. This issue has been resolved by cancelling the prune time limit whenever an IGMP *Join* is received.

PCR: 31013 Module: SWI Level: 2

If ports were set to a speed of 100m when creating a switch trunk, the speed could not subsequently be set to 1000m, even if the ports were capable of that speed. This issue has been resolved.

PCR: 31015 Module: STP Level: 2

The PORT and PORTPRIORITY parameters of the STP PORT command were not always updating switch instances on ports that are members of multiple STP instances. This issue has been resolved.

PCR: 31017 Module: NTP Level: 3

The *RootDispersion* value in NTP packets was negative. RFC 1305 states that only positive values greater than zero are valid. This issue has been resolved.

PCR: 31019 Module: PIM6 Level: 2

The checksum for the PIMv2 *Register* message for IPv6 was not being calculated correctly. This issue has been resolved.

PCR: 031020 Module: PIM Level: 2

When the switch received a generation ID change message, it was not responding by sending a PIM HELLO message. This issue has been resolved.

PCR: 31028 Module: BGP Level: 2

BGP did not always send *Withdrawn* advertisements when a route went down. This issue has been resolved.

PCR: 31036 Module: CORE Level: 4

The output of the SHOW SYSTEM command has been changed on AT-8800 Series switches. The output now includes the status of the temperature and fan. See Figure 2 on page 14 and Table 4 on page 15.

Figure 2: Example output from the SHOW SYSTEM command.

```
Switch System Status                              Time 08:32:23 Date 06-Nov-2003.
Board      ID  Bay Board Name                          Rev    Serial number
-------------------------------------------------------------------------------
Base      148      8848                               P3-7   58476578
-------------------------------------------------------------------------------
Memory -   DRAM : 65536 kB    FLASH : 32768 kB
-------------------------------------------------------------------------------
SysDescription
AT-8848 version 2.6.1-02 30-Oct-2003
SysContact

SysLocation

SysName

SysDistName

SysUpTime
3608 ( 00:00:36 )
Boot Image      : rmb106.fbr size 496544 06-Nov-2003
Software Version: 2.6.1-02 30-Oct-2003
Release Version : 2.6.1-00 20-Aug-2003
Patch Installed : Release patch
Territory       : japan
Help File       : help.hlp

Main PSU        : On
RPS Monitor     : Off

Current Temperature : Normal

Fan     Status
--------------
1       Normal
2       Normal
3       Normal
4       Normal
--------------

Configuration

Boot configuration file: Not set
Current configuration: None

Security Mode   : Disabled

Patch files
Name            Device     Size      Version
-----------------------------------------
86261-02.paz    flash      170996    2.6.1-2
-----------------------------------------
```

Table 4: New parameters displayed in the output of the SHOW SYSTEM command for AT-8800 series switches.

Parameter	Meaning
Current Temperature	The status of the switch's temperature. "Normal" means the switch is operating in the required temperature range. "Warning" means there has been a temperature-related error requiring attention. "Failed" means there was an internal error while reading the temperature.
Fan Status	The status of each of the switch's four fans. "Normal" means the fan is operating as expected. "Warning" means a fan is operating outside the desired range. "Failed" means there was an internal error while reading the fan status.

PCR: 31040 Module: PIM Level: 2

When two devices are BSR candidates, and have the same preference set with the SET PIM BSRCANDIDATE PREFERENCE command, the device with the higher IP address was not elected as the candidate. This issue has been resolved.

PCR: 31041 Module: PIM Level: 3

A *Prune* message sent to an old RP neighbour was ignored when a new unicast route was learned. This issue has been resolved.

PCR: 31042 Module: PIM Level: 3

On Rapier series switches, an *Assert* message was not sent after the prune limit expired. This issue has been resolved.

PCR: 31044 Module: SWI Level: 4

The log message "`IGMP Snooping is active, L3FILT is activated`" has been changed to "`IGMP packet trapping is active, L3FILT is activated`". The revised message is clearer when IGMP is enabled and IGMP snooping is disabled.

PCR: 31052 Module: FIREWALL Level: 3

The following changes have been made to the ADD FIREWALL POLICY RULE and SET FIREWALL POLICY RULE commands:

- An IP address range for the IP parameter is now only accepted when enhanced NAT is configured.
- An IP address range for GBLREMOTE parameter is now only accepted when reverse or reverse-enhanced NAT is configured.
- The GBLIP parameter is not accepted for a public interface when enhanced NAT is configured.

PCR: 31057 Module: SW56 Level: 4

Port link status LEDs on disabled ports were not always operating correctly on AT-8800 Series switches. This issue has been resolved.

PCR: 31058 Module: NTP Level: 3

When the interval between the NTP server and client exceeded 34 years 9 days and 10 hours, the time set on the client was incorrect. This issue has been resolved.

PCR: 31063 Module: IPG Level: 2

MVR was not operating if IGMP had not been enabled. This issue has been resolved.

PCR: 31068 Module: STP Level: 2

A fatal error occurred when the PURGE STP command was executed when STP instances were defined with VLAN members. This issue has been resolved.

PCR: 31071 Module: SWI Level: 4

The warning given when a QoS policy is active on a port operating at reduced speed has been changed to reflect the problem more accurately. The old message was:

```
Warning (2087343): Port <Port num> is currently used in QoS
policy <QoS policy num>, this policy may become incorrect
due to the port bandwidth.
```

The new message is:

```
Warning (2087350): Port <Port num> is operating at less than
its maximum speed: this may affect QoS policy <QoS policy
num>.
```

PCR: 31074 Module: PPP Level: 2

The PPP idle timer was not being updated correctly. This issue has been resolved.

PCR: 31079 Module: SW56 Level: 2

Ports sometimes stopped operating if the port speed was changed while packets still occupied the switching fabric. This issue has been resolved. All packets are now released before changes can be made to port configurations.

PCR: 31080 Module: IPv6 Level: 2

When a ping was sent to the device's link-local address, the device flooded the ICMP *Reply* packet over the VLAN. This issue has been resolved.

PCR: 31082 Module: STP Level: 2

The root bridge did not transmit BPDU messages with changed *hellotime*, *forwarddelay* and *maxage* values. This issue has been resolved.

PCR: 31085 Module: LDAP Level: 3

LDAP could not receive large messages spanning multiple packets. This issue has been resolved.

PCR: 31094 Module: FILE Level: 3

Files with lines over 132 characters in length could not be transferred using TFTP. This limit has now been raised to 1000 characters to match the maximum command line length.

PCR: 31097 Module: SW56 Level: 2

When broadcast packets were transmitted to one of two VLAN interfaces, and a ping was sent to the other interface, 10% of the pings timed out. This issue has been resolved.

PCR: 31099 Module: FIREWALL Level: 4

In the output of SHOW FIREWALL EVENT command, the DIRECTION of denied multicast packets was shown as “out”, not “in”. This issue has been resolved.

PCR: 31102 Module: DHCP Level: 2

When a boot file for DHCP was specified with the ADD DHCP POLICY FILE command, a blank space was added after the filename in the configuration. This meant the file could not be found. This issue has been resolved.

PCR: 31106 Module: MLD Level: 2

When the device received a version 1 *Query* packet, it become a non-querier on that interface, even if it should have remained as the querier. This issue has been resolved.

PCR: 31110 Module: IPV6 Level: 2

When the preference value for RIPng was changed with the SET IPV6 ROUTE PREFERENCE command, the new value was not updated in the IPV6 routing table. This issue has been resolved.

PCR: 31118 Module: SWI Level: 2

When the TYPE parameter was specified for the ADD SWITCH L3FILTER command, the type was sometimes a different value in the device’s hardware table. This issue has been resolved.

PCR: 31122 Module: RMON Level: 3

The *etherHistoryIntervalStart* node in the *etherHistoryTable* showed incorrect values for the first and last 30 second interval periods. This issue has been resolved.

PCR: 31129 Module: IPX2 Level: 2

A fatal error occurred if IPX was disabled and then re-enabled when there was a high rate of incoming IPX traffic on the device. This issue has been resolved.

PCR: 31130 Module: FFS Level: 2

In some circumstances FlashROM was corrupted. This issue has been resolved. FlashROM is now write protected.

PCR: 31137 Module: CORE Level: 4

Rapier Series switches with a DC power supply did not recognise the DC power supply. This issue has been resolved.

Features in 86261-01

Patch file details are listed in Table 5:

Table 5: Patch file details for Patch 86261-01.

Base Software Release File	86-261.rez
Patch Release Date	2-Oct-2003
Compressed Patch File Name	86261-01.paz
Compressed Patch File Size	94120 bytes

Patch 86261-01 includes the following enhancements and resolved issues:

PCR: 03268 Module: SWI Level: 1

When using MVR on a Rapier 48 or Rapier 48*i*, multicast packets were not forwarded correctly between ports 1-24 and 25-48. This issue has been resolved.

PCR: 03524 Module: OSPF, IPG Level: 2

OSPF disabled RIP unless RIP was activated using the SET OSPF RIP command. This issue has been resolved.

PCR: 03798 Module: IKMP Level: 3

ISAKMP did not support the IPSec message option *ID_IPV6_ADDR_SUBNET* (RFC 2407, 4.6.2.7). ISAKMP was using the *ID_IPV6_ADDR* (RFC 2407, 4.6.2.6) option instead. This issue has been resolved.

PCR: 03826 Module: BGP Level: 2

When BGP imported routes from IP with the ADD BGP IMPORT command, and there were multiple import choices, the best IP route was not always imported. This issue has been resolved.

PCR: 03828 Module: IPV6 Level: 2

The MTU value for IPv6 PPP interfaces was always set to 1280 bytes. This MTU value is now correctly set to 1500 bytes, and 1492 bytes for PPP over Ethernet (PPPoE).

PCR: 03836 Module: OSPF Level: 2

OSPF sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03861 Module: IPV6 Level: 2

When a connector was plugged into one physical interface, the RIPng request packet was erroneously transmitted from all interfaces on the switch. This issue has been resolved.

PCR: 03864 Module: BGP Level: 2

BGP sent *Update* packets when the local host route table changed but did not affect BGP. Also, BGP did not send *Withdrawn* packets when there was a change in the best route. These issues have been resolved.

PCR: 03865 Module: FIREWALL Level: 2

When dual firewall policies were defined, public to private passive mode FTP transfers sometimes failed. This issue has been resolved.

PCR: 03867 Module: BGP Level: 2

BGP sometimes chose routes with an infinite metric over routes with a finite metric when selecting the best local route. This issue has been resolved.

PCR: 03875 Module: IPG Level: 2

Sometimes OSPF routes were not entered in the IP route table. This issue has been resolved.

PCR: 03876 Module: PING Level: 2

A fatal error occurred if the TRACE command was executed when a trace was already in progress. This issue has been resolved.

PCR: 03881 Module: SW56 Level: 2

On AT-8800 series switches, if a port was not set to autonegotiate, and the cable was unplugged and then plugged back in, the port stopped sending packets. This issue has been resolved.

PCR: 03882 Module: SW56 Level: 2

When port had a learn limit configured, MAC addresses were not added to the forwarding database. Also, when a MAC address was learned on a port, and then the same address was learned on another port, the forwarding database did not change to the more recently learned port. These issues have been resolved.

PCR: 03883 Module: IPG Level: 3

Some IP addresses were not displayed correctly in log messages. This issue has been resolved.

PCR: 03884 Module: IPG Level: 2

The IGMP MVR membership timeout was not operating correctly. Membership of a multicast group is now eliminated when it times out. Also, *Leave* messages were not being processed correctly, which sometimes delayed the membership timeout. These issues have been resolved.

PCR: 03885 Module: CORE Level: 3

The operation of the FAULT LED on AT-8800 series switches has been modified. Now, if there are multiple faults, resolving one fault will not turn off the LED.

PCR: 03886 Module: SW56 Level: 3

AT-8800 series switches received frames when the physical link was not established. This issue has been resolved.

PCR: 03888 Module: DHCP, TELNET Level: 2

When the device was configured as a DHCP server, a fatal error sometimes occurred when a telnet session to the device was closed while DHCP was reclaiming IP addresses. Also, a telnet error message displayed an incorrect value when a telnet command line parameter was repeated (for example, SHOW TELNET TELNET). These issues have been resolved.

PCR: 03895 Module: DHCP Level: 2

If the DHCP server had a policy name greater than 5 characters long, and a very long MERITDUMP or ROOTPATH value, the device could not correctly create the configuration. This issue has been resolved.

PCR: 03896 Module: TTY Level: 3

A fatal error occurred when a long string of text was pasted over an existing long string of text at the CLI. This issue has been resolved.

PCR: 03898 Module: ETH Level: 3

An ETH interface was sometimes shown as *Up* in the output of the SHOW INTERFACE command when it was actually *Down*. This issue has been resolved.

PCR: 03902 Module: FIREWALL Level: 3

Under some circumstances traffic did not have NAT applied if a standard subnet NAT rule was added to a public interface. Such rules did not correctly match incoming traffic when the REMOTEIP parameter in the ADD FIREWALL POLICY RULE command was not specified, and the destination IP address was not the interface's actual IP address. If this situation occurred, traffic was redirected back out the public interface. This issue has been resolved.

PCR: 03903 Module: SWI Level: 2

Filtering was not working correctly on AT-8848 switches between port groups 1-24, 25-48, and the two GBIC ports. This issue has been resolved.

PCR: 03904 Module: SWI Level: 3

Port mirroring was not working correctly on AT-8848 switches where the source, destination and mirror ports were spread between two or more of the port groups 1-24, 25-48, and the two GBIC ports. This issue has been resolved.

PCR: 03906 Module: SWITCH Level: 2

Software emulation of layer 3 hardware filtering was not operating correctly. Packets that the switch had no routing information for were filtered incorrectly. The first packet of a flow that should have been dropped was not dropped, and a flow that should have been allowed was being dropped. This issue has been resolved.

PCR: 03907 Module: IPV6 Level: 2

The CREATE CONFIG command did not generate the TYPE parameter for ADD IPV6 INTERFACE commands. This issue has been resolved.

PCR: 03909 Module: SCC Level: 2

A fatal error sometimes occurred when encryption is enabled with Frame Relay over a synchronous link. This was due to errors in the synchronous transmit queue when then the transmission of a synchronous frame timed out (because the device started up). This issue has been resolved.

PCR: 03911 Module: SWI Level: 3

The ADD SWITCH FILTER command returned an incorrect error message if a broadcast address was specified for the DESTINATION parameter. This issue has been resolved.

PCR: 03914 Module: IPG, VLAN Level: 3

When IGMP snooping was disabled with the DISABLE IGMPSNOOPING command, IGMP packets were not flooded. This issue has been resolved.

PCR: 03915 Module: CORE, SW56 Level: 2

Installing GBICs in AT-8800 series switches caused an error with the I2C bus. This issue has been resolved.

PCR: 03918 Module: DHCP6 Level: 2

DHCP6 server suffered a fatal error if it received more than 689 requests for temporary addresses. This issue has been resolved.

PCR: 03919 Module: IPV6 Level: 2

A fatal error could occur if pinging a deleted IPv6 interface. This issue has been resolved.

PCR: 03920 Module: L2TP Level: 3

If the LNS was configured without associating a PPP template to an IP address range, the device restarted when the dynamic PPP was created. This issue has been resolved.

PCR: 03921 Module: IP ARP Level: 3

ARP requests with invalid source MAC and IP addresses were being processed, but should have been dropped. This issue has been resolved.

PCR: 03924 Module: IPG Level: 2

The CPU can no longer receive multicast traffic when there are no Layer 3 interfaces configured as static multicast senders.

PCR: 03925 Module: IPV6 Level: 3

Incorrect debug information was returned when an ICMPv6 *PacketTooBig* message was received. This issue has been resolved.

PCR: 03928 Module: IKMP Level: 2

ISAKMP in *aggressive* mode did not establish a connection when the peer client sent 10 or more payloads. This issue has been resolved.

PCR: 03930 Module: FIREWALL Level: 2

A fatal error sometimes occurred when certain types of traffic travelled over a WAN interface connected to the Internet. This issue has been resolved.

PCR: 03931 Module: IPSEC Level: 3

The IPSec configuration was not created correctly when the RADDRESS and LNAME parameters in the CREATE IPSEC POLICY command were used together. This issue has been resolved.

PCR: 03933 Module: SW56, SWI Level: 2

When a Rapier rebooted while a GBIC port was receiving broadcast packets, some copper GBICs did not send packets after the switch booted up. Also, when a copper GBIC received pause frames on a Rapier, it did not stop sending packets. These issues have been resolved.

PCR: 03934 Module: IPSEC Level: 2

The CREATE IPSEC POLICY command failed if the interface specified with the INTERFACE parameter did not have a global IPv6 interface defined. This PCR implements a workaround by using the interface's link-local IPv6 address if no other IPv6 address can be found.

PCR: 03936 Module: IKMP Level: 3

When ISAKMP was used with IPv6, an incorrect IP address was displayed in the output of the SHOW ISAKMP EXCHANGE command. This issue has been resolved.

PCR: 03938 Module: IKMP Level: 3

DHEXPONENTLENGTH parameter in the CREATE ISAKMP POLICY command was not accepted when creating ISAKMP policies that used IPv6. This issue has been resolved.

PCR: 03939 Module: IPV6 Level: 2

When a *NeighbourAdvert* message containing an anycast target address was received, the device incorrectly performed Duplicate Address Detection. This issue has been resolved.

PCR: 03942 Module: SW56 Level: 2

IP multicasting was not operating correctly across all ports on an AT-8848 switch. This issue has been resolved.

PCR: 03946 Module: IPSEC Level: 3

When IPSec was used with IPv6, an incorrect IP address was displayed in the output of the SHOW IPSEC SA command. This issue has been resolved.

PCR: 03949 Module: IPSEC Level: 3

If a local IP address and remote IP address were not specified in the CREATE IPSEC POLICY command for IPv6 IPSec, the SET IPSEC POLICY configuration was shown unnecessarily in the output of the SHOW CONFIG DYNAMIC=IPSEC command. This issue has been resolved.

PCR: 03952 Module: SWI Level: 3

MAC address are now deleted from the all the internal tables for ports where the learn limit has been exceeded.

PCR: 03953 Module: SW56 Level: 3

On AT-8800 series switches, strict QoS scheduling is now enforced for ports where egress rate limiting is applied. On Rapier *i* series switches, the same QoS setup is now applied to all of the appropriate ports when setting up egress rate limiting.

PCR: 03969 Module: IPG Level: 2

When saving the IP filter configuration, non-default values for the source IP address mask were not always saved correctly. This issue has been resolved.

PCR: 03976 Module: SW56 Level: 3

On AT-8800 series switches, if a port was set to use 10 Mbps full duplex with the SET SWITCH PORT SPEED=10MBFULL command, there was a delay before the port was set. This delay has been minimised.

PCR: 03979 Module: CORE Level: 3

On AT-8800 series switches, the temperature at which a temperature alarm is generated has been increased.

PCR: 31037 Module: SW56 Level: 2

Uplink modules on Rapier series switches sometimes did not enable a link correctly. This issue has been resolved.

Availability

Patches can be downloaded from the Software Updates area of the Allied Telesyn web site at *www.alliedtelesyn.co.nz/support/updates/patches.html*. A licence or password is not required to use a patch.